HRCDC
Health Research Consent Declaration Committee

HRCDC Data Breach Protocol

Title	Data Breach - Public
Document Type	Protocol
Reference / Version	1.0
Status	Final
Last updated	05.06.2019
Sign off	Pending
Background	This policy applies to the HRCDC, the Secretariat and other persons engaged in activities relating to HRCDC on a permanent or temporary basis (hereinafter referred to as "Data Users").

1. Overview

1.1 The purpose of this document is to provide guidance on the process that must take place should a Data Breach (as defined in Section 1.2) occur.

1.2 Further details on the HRCDC's policy regarding data protection and privacy can be found in the HRCDC Privacy Policy.

2. What to do in case of a breach

2.1 The HRCDC has put in place a security breach management team ("SB Team"), its members are HRCDC Chairperson and Secretariat (Programme Manager and Project Officer). Please report to the Chair via the Secretariat in relation to a Data Breach.

2.2 Where a Data Breach has occured and is identified by a Data User, there are two options to report a breach;

- Call: (01) 2345179 (Programme Manager); or
  (01) 2345257 (Project Officer)
- Email: dpo@hrcdc.ie

Typical breaches include situations where an individual's data is sent to another individual, e.g. two letters in one envelope, lost laptop, iPad or mobile device and a cyberattack ("Data Breach").

2.3 The SB Team has been trained to understand their role in managing a Data Breach. Dealing with a Data Breach quickly can limit the damage that it causes.

3. Investigate the facts

3.1 Our SB team will investigate what happened to determine:

- The nature and cause of the Data Breach; and
- The extent of the damage or harm that results, or could result, from the Data Breach.

3.2 The reporting Data User will be directed to complete a data breach questionnaire on a GDPR portal. This reporting process will be facilitated by the SB Team

4. Stop or mitigate the breach

4.1 The SB team will take action to stop the Data Breach from continuing or recurring and mitigate the harm that may continue to result from the Data Breach. It will consider the following:

4.2 What steps can be taken to stop or minimise further loss?

4.3 What steps can be taken to recover, correct or delete data?

4.4 Does evidence need to be preserved for a potential criminal investigation?

4.5 If the Data Protection Commissioner ("DPC") is notified or becomes involved in the Data Breach, he/she will want to know what has been done to stop or mitigate the breach and what the HRCDC will do to ensure future compliance with the security principal in the Data Protection Act 1988 and 2003, as amended (the "DPA"), and the EU General Data Protection Regulation (the "GDPR"). The DPC has powers to obtain information and take enforcement action if necessary.

4.6 It is important that all steps taken when dealing with a Data Breach are documented so that an accurate record of events can be maintained.

5. Insurance

5.1 The SB team will check criminal insurance and professional indemnity insurance policies or any other relevant policy and consider whether notification is required.

6. Create a detailed assessment of the Data Breach

6.1 Record-keeping and assessment is the next important step. The SB team may ask you to fill out a detailed data breach assessment form. It is important that this is completed accurately and speedily.

7. Consider who needs to be notified

7.1 The SB team will need to consider who (if anyone) should be notified of the Data Breach. These could include:

i. **Data subjects:** Data subjects may need to be notified that their data has been compromised and given details of the Data Breach, what steps HRCDC has taken to mitigate the Data Breach and any potential repercussions for the data subject.

ii. **The DPC:** The DPA requires notification to the DPC in the event of a data security breach unless certain exemptions apply. In general, the Data Breach will require notification to the DPC if the data includes:

- the possibility of harm to the data subjects
- a large volume of personal data
- sensitive data (e.g. financial or health information)

iii. **Other Data controllers:** If there are other data controllers of the personal data in question, they may be notified (although this is not a legal obligation under the DPA). We may need to notify other data controllers under the terms of the contract with that data controller or under the requirements of the GDPR;

iv. **The Gardaí:** if the Data Breach involved a potentially criminal act, then the Gardaí or other law enforcement agencies may need to be notified;

v. **Regulators**: some professional regulators may need to be informed of the Data Breach within their remit.

7.2 The SB team will take appropriate legal advice and public relations advice as soon as possible and generally in advance of making notification. Common sense should be applied in permitting delay where the Data Breach requires immediate notification to those affected for the health or personal safety of the data subjects.

7.3 The SB Team will always notify the Data Controller/Processors of a Data Breach.

8. Audit of security appropriateness and the need to make necessary improvements

8.1 Following a Data Breach, an investigation will take place and include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed.

8.2 Where one or more data processors may have caused the Data Breach, the SB team will consider whether adequate measures were in place to comply with security.

8.3 Where security is found not to be appropriate, the SB team will consider what action needs to be taken to raise data protection and security compliance standards. If the DPC is notified or becomes involved in the Data Breach, this information may be requested.

8.4 The above process will be documented by the SB team for the purpose of the HRCDC's data protection records.